CYBER RESILIENCE ACT

Policy briefing

Weblink	http://data.europa.eu/eli/reg/2024/2847/oj
Relevance	☐ National policy ☐ EU policy X other: Regulation (EU)
Briefing done by	Peppy Florou

Short summary of the policy

The **Cyber Resilience Act (2024/2847)** is a regulation designed to improve the cybersecurity of products with digital elements throughout their lifecycle. It mandates that manufacturers integrate cybersecurity measures during the design phase and ensure ongoing security through regular updates and vulnerability management. The regulation applies to a wide range of products, including both hardware and software, and sets clear requirements for vulnerability disclosure, risk assessment, and product monitoring. Manufacturers must also ensure secure disposal of products. Market surveillance measures are introduced to ensure compliance, and penalties are set for non-compliance (notably, fines or restrictions on market access for non-compliant products).

By establishing these standards, the Act aims to protect users from cybersecurity threats, reduce vulnerabilities in digital products, and increase trust in the digital ecosystem across the EU. Additionally, it addresses the issue of "security by design," ensuring that cybersecurity is an integral part of product development. The Act also requires manufacturers to implement effective risk management processes and take necessary actions to reduce potential cybersecurity risks associated with their products. For example, a manufacturer of IoT devices will need to integrate automatic security updates and a system for reporting vulnerabilities.

This regulation enhances the EU's overall cyber resilience by ensuring that digital products and services are secure and that risks are managed proactively. Through its comprehensive approach, the Cyber Resilience Act aligns with broader EU cybersecurity efforts, aiming to safeguard the European digital single market against increasing cyber threats.

By focusing on securing the entire lifecycle of digital products and enhancing the response to emerging vulnerabilities, the Cyber Resilience Act represents a significant step forward in establishing a robust and secure digital environment. It is particularly focused on protecting critical sectors and consumers, ensuring that cybersecurity is maintained at every stage of product use, from deployment to decommissioning.

The DEP4ALL project is funded by the European Commission under the Digital Europe Programme, under grant agreement no. 101167919. Any opinions expressed in these pages are those of the author/organisation and do not necessarily reflect the views of the European Commission.

Main objectives of the policy

The main objectives of the **Cyber Resilience Act** (CRA) are:

- **Enhance cybersecurity** for products with digital elements throughout their lifecycle.
- **Ensure secure design** and development of products, integrating cybersecurity from the start.
- **Regular updates and vulnerability management** to address emerging threats.
- **Mandatory disclosure of security vulnerabilities** to users and authorities.
- **Improve market surveillance** to ensure compliance and address non-compliant products.
- **Strengthen EU resilience** by protecting users and sectors from cybersecurity risks.
- **Increased awareness** of the cybersecurity of digital products for end users and businesses.

Context and relation to the Digital Europe Programme (DEP)

The **Cyber Resilience Act** aligns closely with DEP which focuses on bolstering Europe's digital capabilities and infrastructure. DEP aims to advance areas such as cybersecurity, high-performance computing, and artificial intelligence, all of which benefit from the CRA's focus on secure digital product design. Specifically, the CRA:

- **Supports DEP's Cybersecurity Objectives**: By mandating security-by-design principles, the CRA reinforces DEP's goal of enhancing EU-wide cybersecurity infrastructure and resilience.
- **Facilitates Market Development**: The CRA's harmonized rules complement DEP's investment in building a competitive digital single market, ensuring safer products and boosting consumer trust.
- **Addresses Skills Gaps**: DEP's initiatives to develop a skilled digital workforce are essential for implementing CRA's provisions, as the Act depends on professional expertise to achieve compliance.
- **Enhances Strategic Autonomy**: Both initiatives aim to reduce Europe's reliance on external suppliers by fostering local innovation and leadership in secure digital technologies.

By integrating with DEP, the CRA strengthens the EU's vision for a resilient, inclusive, and competitive digital ecosystem, essential for achieving the objectives of Europe's Digital Decade.

Parts of the policy directly related to specific objectives (SO) in DEP

The Cyber Resilience Act aligns with several SOs of DEP by addressing key areas of cybersecurity, digital trust, and technology resilience:

SO1: High Performance Computing (HPC)

CRA's security standards can benefit from HPC technologies in the development and testing of secure digital products, enabling better performance in threat analysis and mitigation. Projects involving HPC for cybersecurity can help meet CRA compliance, aligning with DEP's support for high-performance computing solutions.

SO2: AI Continent

The CRA encourages the use of AI for enhancing product security and vulnerability detection. AI-driven cybersecurity solutions can assist in meeting CRA's secure-by-design requirements, benefiting DEP's AI focus.

SO3: Cybersecurity and Trust

The CRA directly supports this objective by setting cybersecurity requirements for digital products, ensuring their trustworthiness across sectors. Proposals that strengthen cybersecurity solutions are key to aligning with CRA mandates and DEP goals in trust-building and EU-wide security.

SO4: Advanced Digital Skills

The CRA emphasizes the need for a skilled workforce to ensure compliance with cybersecurity standards. Proposals focused on cybersecurity training and certification will align with both DEP and CRA objectives, addressing the growing skill gap.

SO5: Deployment and Best Use of Digital Capacities and Interoperability

The CRA promotes secure, interoperable products that align with EU standards for digital infrastructure. Proposals developing secure, interoperable solutions will support both the CRA and DEP objectives of enhancing digital infrastructure.

Activities in the DEP Work Programme 2025-27 contributing to the objectives of the policy

These open and forthcoming calls support the implementation of the CRA, particularly in areas related to SME preparedness, product security capacity, and conformity assessment readiness.

Uptake of innovative cybersecurity solutions for SMEs
Supports SMEs in adopting and deploying innovative cybersecurity solutions that enhance their security posture, resilience, and competitiveness. Strengthening SME technical capabilities, facilitating compliance readiness, and reducing the number of vulnerable digital products entering the EU market will support the implementation of the CRA.

SECURE-CALL #1 - SECURE First Open Call For Proposals - **Cascade funding**
EU funded project: SECURE - Strengthening EU SMEs Cyber Resilience, GA**:** 101190325
Supports cybersecurity innovation, testing, validation, and deployment activities through cascade funding, particularly targeting SMEs and emerging technology providers. Supports CRA objectives by fostering innovation aligned with product security requirements and strengthening the European cybersecurity ecosystem.

Cyber Resilience Boost: Supporting capacity building for cyber resilience of products II. - **Cascade funding; EU funded project:** TEST-CERT-CZ - Building Testing and Certification Capabilities in the Czech Republic, GA: 101127940
Strengthen testing, certification, and product cybersecurity capacity, supporting organisations in enhancing the resilience and compliance of digital products. Supports CRA implementation by expanding testing and certification infrastructure, enhancing SME readiness for conformity assessments, and reducing implementation bottlenecks.

Related policies and further information

NIS2 Directive: Establishes measures to achieve a high common level of cybersecurity across the Union. NIS2 strengthens organizational cybersecurity and supervisory frameworks, while the CRA addresses cybersecurity requirements for products with digital elements placed on the Union market.

Cybersecurity Act: Establishes a European cybersecurity certification framework for ICT products, ICT services and ICT processes, and strengthens the mandate of the EU Agency for Cybersecurity (ENISA).

The DEP4ALL project is funded by the European Commission under the Digital Europe Programme, under grant agreement no. 101167919. Any opinions expressed in these pages are those of the author/organisation and do not necessarily reflect the views of the European Commission.

Cyber Solidarity Act: Establishes measures to strengthen solidarity and operational capacities across the Union to detect, prepare for and respond to significant and large-scale cybersecurity threats and incidents.

Digital Operational Resilience Act (DORA): Establishes uniform requirements concerning ICT risk management, incident reporting, digital operational resilience testing, and oversight of ICT third-party service providers for financial entities.

Artificial Intelligence Act: Addresses safety, fundamental rights and risk governance aspects of AI systems, including robustness and cybersecurity safeguards for high-risk AI systems.

EU Cybersecurity Strategy: Sets the strategic direction for strengthening cybersecurity resilience, technological sovereignty and operational capacity across the Union.

For related events, please check out the online calendars: Shaping Europe's digital future, ECCC

The DEP4ALL project is funded by the European Commission under the Digital Europe Programme, under grant agreement no. 101167919. Any opinions expressed in these pages are those of the author/organisation and do not necessarily reflect the views of the European Commission.